

Vuln Live List Update

Slack & Web Service

중부대학교 정보보안SW융합전공
김두형, 은정욱, 박형준

2022.07.28

- 팀원 소개
- 프로젝트 개요
- Overview
- Service Status[Slack, Web]
- Demo
- 개선 사항 및 계획



김두형

- 팀장
- Web Service
- Slack WebHook API



은정욱

- CVE Crawler Develop
- Slack WebHook API



박형준

- CVE Crawler Develop
- Slack WebHook API

- CVE = Common Vulnerabilities and Exposures
- 정보보안 취약점 표준 코드(CVE ID번호 할당)
 - ↳ CVE - 2022 - 23100

취약점 공개되면 15분 내에 해커들의 스캔 시작된다

좋아요 17개 | 입력 : 2022-07-27 12:31



#정보보호 #정보보안 #IT보안 #사이버보안 #취약점 #패치 #스캔

취약점 소식에 민감한 해커들, 한 번 소식 풀리면 몰려 들어 익스플로잇 시도

요약 : IT 외신 블리핑컴퓨터에 의하면 보안 취약점이 하나 공개되면 공격자들의 스캔이 15분 이내에 시작된다고 한다. 보안 업체 팔로알토(Palo Alto Networks)가 발표한 보고서를 인용한 것으로, 이에 의하면 해커들은 항상 새로운 취약점 소식에 귀를 기울이며, 소식이 나오자마자 곧바로 실험에 돌입한다고 한다. 즉 취약점 패치를 여유롭게 할 상황이 아니라는 것이다. 스캔 자체가 위협이 되지는 않지만 그만큼 공격자들이 취약점 소식에 민감하게 반응한다는 것은 분명하다. 스캔 후 그들이 어떤 결론을 내리는 지에 따라 추가 공격이 이어질 수도 있다.

[이미지 = utoimage]

배경 : 인터넷 스캔은 그 자체로 어려운 기술이 아니며, 모든 해킹의 기초 작업을 이룬다. 이제 막 해킹을 배운 사람도 스캔은 얼마든지 할 수 있다. 공격자들이 실시하는 스캔의 주요 목적은 패치가 되지 않은 시스템을 찾아내는 것이다. 후속 익스플로잇이 이어질 가능성이 매우 높다.

말말말 : “CVE-2022-1388 취약점의 경우 올해 5월 4일에 발견됐는데, 취약점 공개 이후 10시간 만에 스캔 및 익스플로잇 시도 행위가 2552번 탐지됐습니다. 먹이 하나에 벌떼처럼 몰려드는 해커들을 쉽게 상상할 수 있습니다.” -해커뉴스-

https://www.boanews.com/media/view.asp?id=108674&kind=1&search=title&find=%C3%EB%BE%E0%C1%A1

"1년 사이 2배 이상" 제로데이 취약점이 점점 더 많이 발견되는 이유

Andrada Fiscutean | CSO | 2022.07.04

지난 1년 반 동안 다양한 유형의 위협 행위자가 수많은 제로데이(zero-day) 취약점을 악용했다. 제로데이 취약점은 소프트웨어 개발자에게 알려지지 않은 것으로, 주로 국가가 후원하는 단체와 랜섬웨어 공격 단체가 악용하고 있다.



© Getty Images Bank

구글 프로젝트 제로(Google Project Zero)는 올 상반기에 20여 가지의 제로데이 취약점을 발견했다. 대부분은 마이크로소프트, 애플, 구글이 개발한 제품에서 발견된 것이고 브라우저와 운영체제의 제로데이가 큰 비중을 차지한다. 6월 7일 아틀라시안의 **컨플루언스 서버(Confluence Server)**에서 발견된 치명적인 REC(Remote Code Execution) 취약점도 계속 악용되고 있는 상황이다.

2021년 발견된 제로데이 취약점의 수는 훨씬 많았다. 구글 프로젝트 제로는 2021년에만 **58가지의 취약점**을 발견했다. 맨디언트가 발견한 제로데이 취약점은 80가지였는데, 2020년보다 2배 이상 많았다. 맨디언트 수석 애널리스트 제임스 새도스키는 “발견되는 모든 제로데이는 발생할 수 있는 공격에 대한 이해를 넓히고 같거나 다른 기술에서 유사한 취약점을 찾아내는 데 도움이 된다. 더 많이 볼수록 더 많이 검출할 수 있다”라고 말했다.

제로데이 취약점 공격은 국가 후원을 받는 공격 단체가 주도하고 있지만, 일반적인 사이버 범죄자들도 만만치 않게 악용한다. 맨디언트에 따르면, 2021년 제로데이 취약점을 악용한 위협 행위자 3명 중 1명은 금전적인 동기를 지니고 있었다. 제로데이 취약점 공격 증가와 다양한 유형의 위협 행위자는 규모에 관계없이 기업에는 우려의 대상이다. 다른 관점에서는 보안 업계에 귀중한 학습 기회를 제공한다.

https://www.itworld.co.kr/topnews/243019

PROCESS

Project OverView - CVE

05

Search Results

There are **104** CVE Records that match your search.

Name	Description
CVE-2022-25154	A DLL hijacking vulnerability in Samsung portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows 7, 10, or 11 to exploit this vulnerability.)
CVE-2021-33114	Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in Windows 10 and 11 may allow an authenticated user to potentially enable denial of service via adjacent access.
CVE-2021-33113	Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.
CVE-2021-33110	Improper input validation for some Intel(R) Wireless Bluetooth(R) products and Killer(TM) Bluetooth(R) products in Windows 10 and 11 before version 22.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-26472	In VembuBDR before 4.2.0.1 and VembuOffsiteDR before 4.2.0.1 installed on Windows, the http API located at /consumerweb/secure/download.php. Using this command argument an unauthenticated attacker can execute arbitrary OS commands with SYSTEM privileges.
CVE-2021-20741	Cross-site scripting vulnerability in Hitachi Application Server Help (Hitachi Application Server V10 Manual (Windows) version 10-11-01 and earlier and Hitachi Application Server V10 Manual (UNIX) version 10-11-01 and earlier) allows a remote attacker to inject an arbitrary script via unspecified vectors.
CVE-2021-0183	Improper Validation of Specified Index, Position, or Offset in Input in software for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0179	Improper Use of Validation Framework in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0178	Improper input validation in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0177	Improper Validation of Consistency within input in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0176	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable denial of service via local access.
CVE-2021-0175	Improper Validation of Specified Index, Position, or Offset in Input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0174	Improper Use of Validation Framework in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0173	Improper Validation of Consistency within input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0172	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2021-0171	Improper access control in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an authenticated user to potentially enable information disclosure via local access.

Windows 11


Search Results

There are **4633** CVE Records that match your search.

Name	Description
CVE-2022-36375	Authenticated (high role user) WordPress Options Change vulnerability in Biplob Adhikari's Tabs plugin <= 3.6.0 at WordPress.
CVE-2022-34853	Multiple Authenticated (contributor or higher user role) Persistent Cross-Site Scripting (XSS) vulnerabilities in wpWax Team plugin <= 1.2.6 at WordPress.
CVE-2022-34839	Authentication Bypass vulnerability in CodexShaper's WP OAuth2 Server plugin <= 1.0.1 at WordPress.
CVE-2022-34650	Multiple Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerabilities in wpWax Team plugin <= 1.2.6 at WordPress.
CVE-2022-34487	Unauthenticated Arbitrary Option Update vulnerability in biplot018's Shortcode Addons plugin <= 3.0.2 at WordPress.
CVE-2022-33969	Authenticated WordPress Options Change vulnerability in Biplob Adhikari's Flipbox plugin <= 2.6.0 at WordPress.
CVE-2022-33965	Multiple Unauthenticated SQL Injection (SQLi) vulnerabilities in Osamaesh WP Visitor Statistics plugin <= 5.7 at WordPress.
CVE-2022-33960	Multiple Authenticated (subscriber or higher user role) SQL Injection (SQLi) vulnerabilities in Social Share Buttons by Supsysyic plugin <= 2.2.3 at WordPress.
CVE-2022-33901	Unauthenticated Arbitrary File Read vulnerability in MultiSafepay plugin for WooCommerce plugin <= 4.13.1 at WordPress.
CVE-2022-33198	Unauthenticated WordPress Options Change vulnerability in Biplob Adhikari's Accordions plugin <= 2.0.2 at WordPress.
CVE-2022-33191	Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Chinmoy Paul's Testimonials plugin <= 3.0.1 at WordPress.
CVE-2022-32289	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.0 at WordPress leading to popup status change.
CVE-2022-32280	Authenticated (contributor or higher user role) Stored Cross-Site Scripting (XSS) vulnerability in Xakuro's XO Slider plugin <= 3.3.2 at WordPress.
CVE-2022-31475	Authenticated (custom plugin role) Arbitrary File Read via Export function vulnerability in GiveWP's GiveWP plugin <= 2.20.2 at WordPress.
CVE-2022-30998	Multiple Authenticated (subscriber or higher user role) SQL Injection (SQLi) vulnerabilities in WooPlugins.co's Homepage Product Organizer for WooCommerce plugin <= 1.1 at WordPress.
CVE-2022-30536	Authenticated Stored Cross-Site Scripting (XSS) vulnerability in Florent Mallefaud's WP Maintenance plugin <= 6.0.7 at WordPress.
CVE-2022-30337	Cross-Site Request Forgery (CSRF) vulnerability in JoomUnited WP Meta SEO plugin <= 4.4.8 at WordPress allows an attacker to update the social settings.
CVE-2022-29923	Authenticated (admin or higher user role) Reflected Cross-Site Scripting (XSS) vulnerability in ThingsForRestaurants Quick Restaurant Reservations plugin <= 1.4.1 at WordPress.
CVE-2022-29495	Cross-Site Request Forgery (CSRF) vulnerability in Sygnoos Popup Builder plugin <= 4.1.11 at WordPress allows an attacker to update plugin settings.
CVE-2022-29454	Cross-Site Request Forgery (CSRF) vulnerability in WordPlus Better Messages plugin <= 1.9.9.148 at WordPress allows attackers to upload files. File attachment to messages must be activated.
CVE-2022-29453	Cross-Site Request Forgery (CSRF) vulnerability in API KEY for Google Maps plugin <= 1.2.1 at WordPress leading to Google Maps API key update.

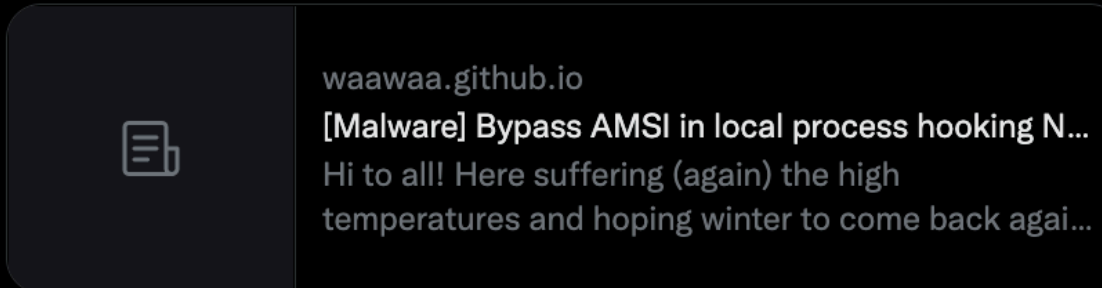
WordPress

Binni Shah @binitamshah · 4시간
RedGuard : a C2 front flow control tool, Can avoid Blue Teams, AVs, EDRs check : github.com/wikiZ/RedGuard




2 16 43

Binni Shah @binitamshah · 3시간
Bypass AMSI in local process hooking NtCreateSection : waawaa.github.io
[Malware] Bypass AMSI in local process hooking NtCreateSection
Hi to all! Here suffering (again) the high temperatures and hoping winter to come back again...

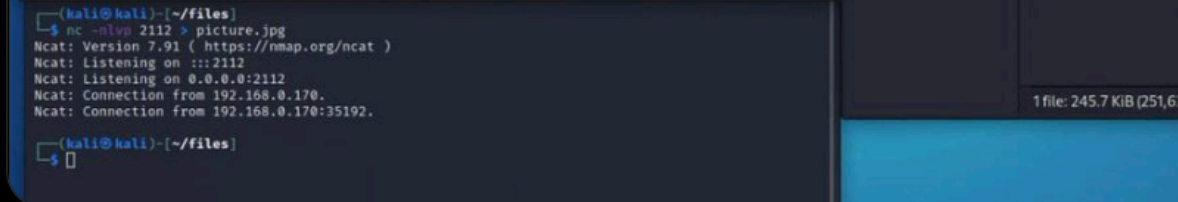
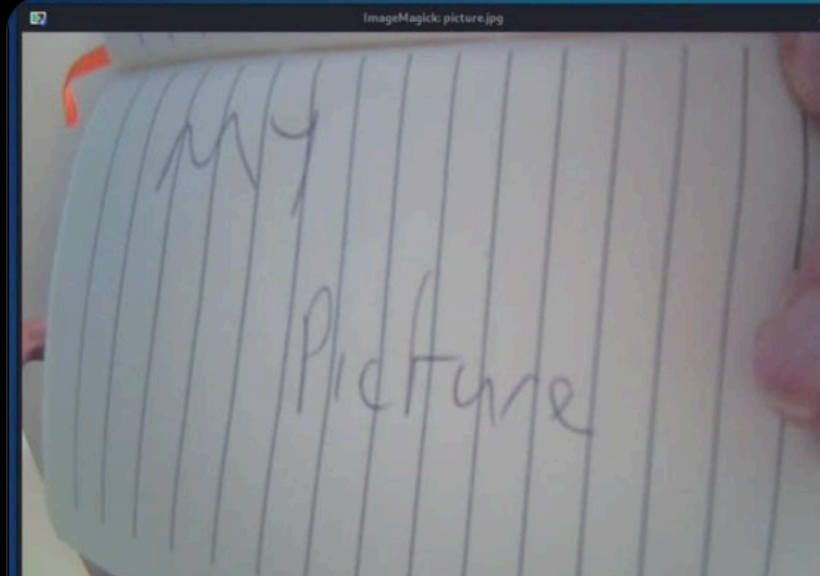


4 15

Binni Shah @binitamshah · 3시간
DeimosC2 : a Golang command and control framework for post-exploitation (It leverages multiple communication methods in order to control machines that have been compromised) : github.com/DeimosC2/DeimosC2 credits @paragonsec @CharlesDardaman @BlaiseBrignac




haxradio.eth @haxradio · 5시간
Flaws in #Enabot Ebo Air Home Security Robot Allowed Attackers to Spy on Users
#IoT #Oday #hacks




3

Oday Exploit Database @inj3ct0r · 9시간
#Oday #MartyMarketplace Multi Vendor Ecommerce Script 1.2 #SQLi #Injection #Vulnerability Oday.today/exploit/description

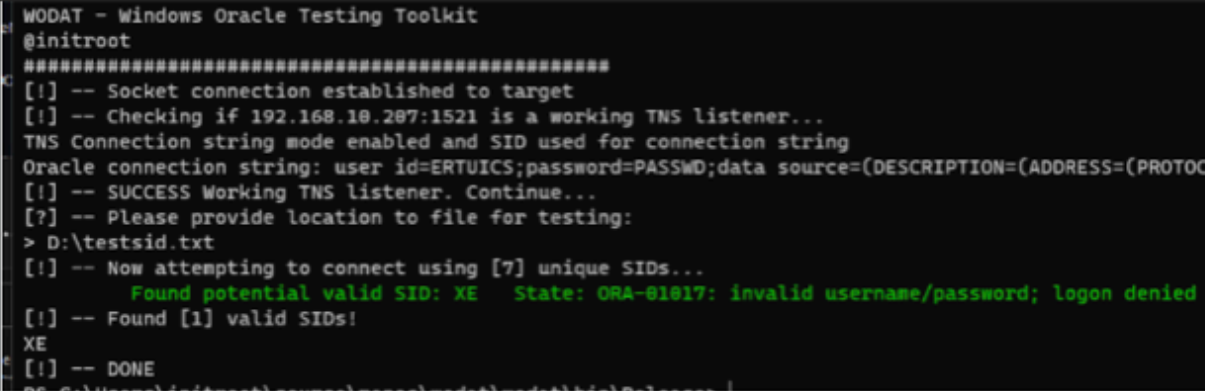


1 1 1

Peter J.M. Simons @peterjmsimons · 17시간
Hackers exploited #PrestaShop zero-day to breach online stores buff.ly/3ctbqv1 by @BleepinComputer
#Oday

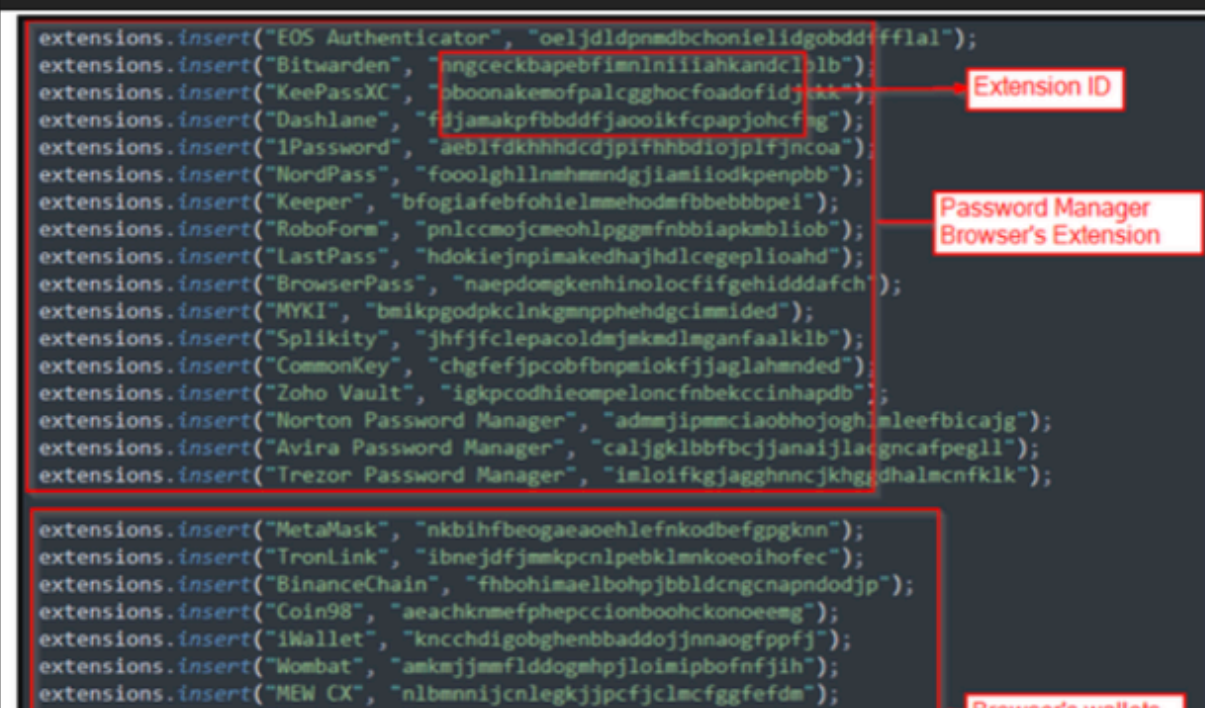


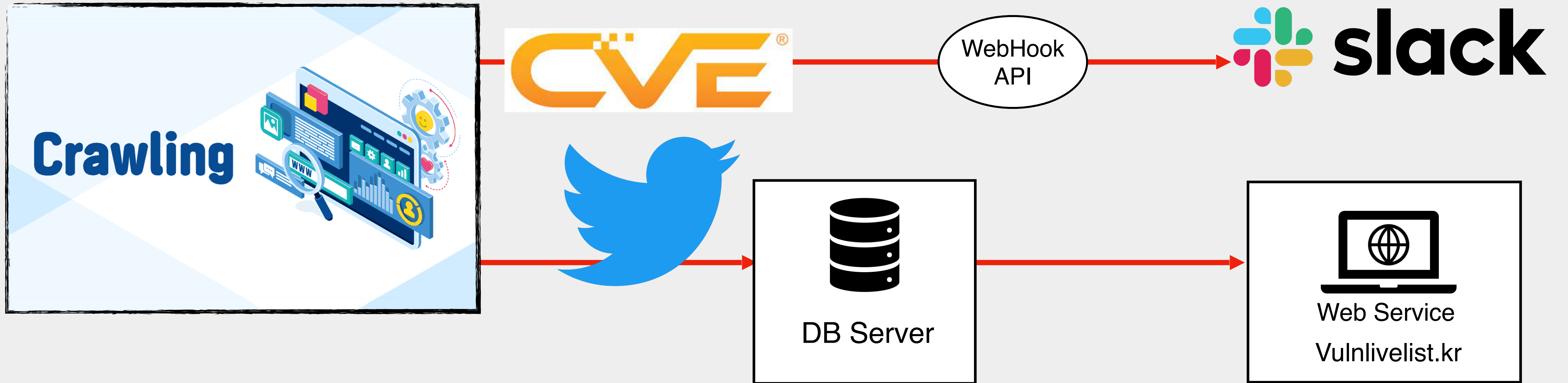
ExploitWareLabs
wodat - Windows Oracle Database Attack Tool
<https://github.com/initroot/wodat>



126 댓글 2개 공유 32회

ExploitWareLabs
9시간 ·
Source code for Rust-based info-stealer released on hacker forums
https://www.bleepingcomputer.com/.../source-code-for-...

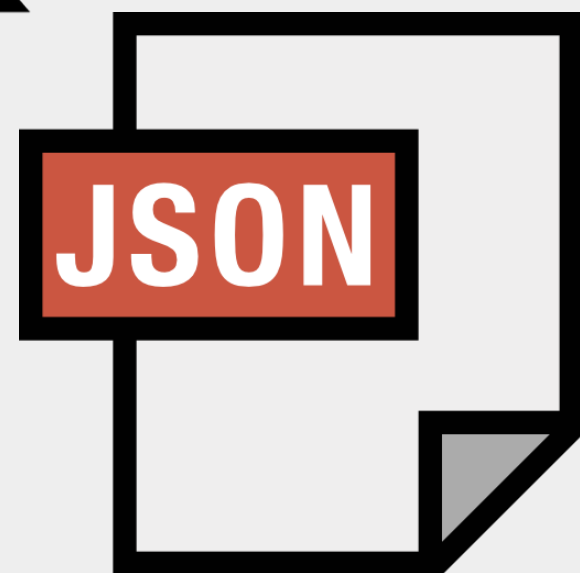




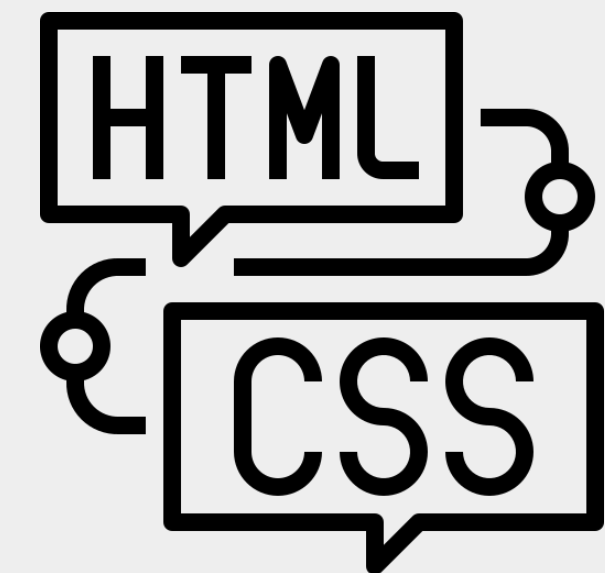
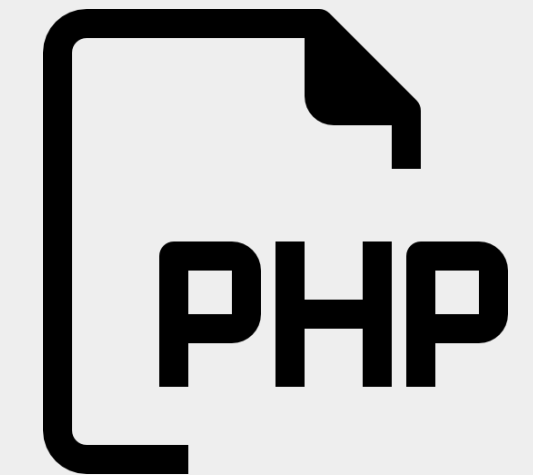
Crawler+ WebHook



slack



Web Service




- WebHook API를 통해 Slack으로 전송
- CVE number data link

Vuln Bot 오후 4:38
New vulnerability information.

CVE-2022-36415

A DLL hijacking vulnerability exists in the uninstaller in Scooter Beyond Compare 1.8a through 4.4.2 before 4.4.3 when installed via the EXE installer. The uninstaller attempts to load DLLs out of a Windows Temp folder. If a standard user places malicious DLLs in the C:\Windows\Temp\ folder, and then the uninstaller is run as SYSTEM, the DLLs will execute with elevated privileges.



[간략히 보기](#)

2022-07-28 04:38:35


상세한 내용은 자세히 보기를 클릭해주세요. [자세히 보기](#)

[간략히 보기](#)

New vulnerability information.

CVE-2022-36900

Jenkins Compuware zAdviser API Plugin 1.0.3 and earlier does not restrict execution of a controller/agent message to agents, allowing attackers able to control agent processes to retrieve Java system properties.



2022-07-28 04:39:12

상세한 내용은 자세히 보기를 클릭해주세요. [자세히 보기](#)

[간략히 보기](#)

New vulnerability information.

CVE-2022-26034



Back

Windows AD(Active Directory)

AD는 사용자가 마이크로소프트 IT 환경에서 업무를 수행하는 데 도움을 주는 데이터베이스이자 서비스 집합입니다. **DB**는 환경에 대한 중요한 정보를 담고 있습니다. 사용자와 컴퓨터 목록, 누가 무엇을 할 수 있는지에 대한 정보 등이 포함됩니다. **Service**는 IT 환경에서 일어나는 대부분의 활동을 제어합니다. 특히 서비스는 일반적으로 사용자가 입력하는 사용자 ID와 비밀번호를 확인하는 방법으로, 사용자가 주장하는 본인이 맞는지 검증하고, 각기 허용된 데이터에만 액세스할 수 있도록 합니다.

AD(Active Directory)

- CVE-2022-26034
Improper authentication vulnerability in the communication protocol provided by AD (Automation Design) server of CENTUM VP R6.01.10 to R6.09.00, CENTUM VP Small R6.01.10 to R6.09.00, CENTUM VP Basic R6.01.10 to R6.09.00, and B/M9000 VP R8.01.01 to R8.03.01 allows an attacker to use the functions provided by AD server. This may lead to leakage or tampering of data managed by AD server.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26034>
- CVE-2022-22975
An issue was discovered in the Pinniped Supervisor with either LADIdentityProvider or ActiveDirectoryIdentityProvider resources. An attack would involve the malicious user changing the common name (CN) of their user entry on the LDAP or AD server to include special characters, which could be used to perform LDAP query injection on the Supervisor's LDAP query which determines their Kubernetes group membership.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22975>
- CVE-2022-22323
IBM Security Identity Manager (IBM Security Verify Password Synchronization Plug-in for Windows AD 10.x) is vulnerable to a denial of service, caused by a heap-based buffer overflow in the Password Synch Plug-in. An authenticated attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 218379.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22323>
- CVE-2022-22154
In a Junos Fusion scenario an External Control of Critical State Data vulnerability in the Satellite Device (SD) control state machine of Juniper Networks Junos OS allows an attacker who is able to make physical changes to the cabling of the device to cause a denial of service (DoS). An SD can get rebooted and subsequently controlled by an Aggregation Device (AD) which does not belong to the original Fusion setup and is just connected to an extended port of the SD. To carry out this attack the attacker needs to have physical access to the cabling between the SD and the original AD. This issue affects: Juniper Networks Junos OS 16.1R1 and later versions prior to 18.4R3-S10; 19.1 versions prior to 19.1R3-S7; 19.2 versions prior to 19.2R3-S4. This issue does not affect Juniper Networks Junos OS versions prior to 16.1R1.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22154>
- CVE-2022-0901
The Ad Inserter Free and Pro WordPress plugins before 2.7.12 do not sanitise and escape the REQUEST_URI before sanitising it. This could allow an attacker to bypass the sanitisation and inject arbitrary code into the page.

Back

PHP

주로 HTML 코드를 프로그래밍적으로 생성하고, 서버쪽에서 실행 되는 프로그래밍 언어이다. 웹에 최적화되어있고, 거의 모든 DB지원한다.

PHP Version

- CVE-2022-34971
An arbitrary file upload vulnerability in the Advertising Management module of Feehi CMS v2.1.1 allows attackers to execute arbitrary code via a crafted PHP file.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34971>
- CVE-2022-34965
OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component /ossn/administrator/com_installer. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34965>
- CVE-2022-32420
College Management System v1.0 was discovered to contain a remote code execution (RCE) vulnerability via /College/admin/teacher.php. This vulnerability is exploited via a crafted PHP file.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32420>
- CVE-2022-32409
A local file inclusion (LFI) vulnerability in the component codemirror.php of Portal do Software Publico Brasileiro i3geo v7.0.5 allows attackers to execute arbitrary PHP code via a crafted HTTP request.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32409>
- CVE-2022-31626
In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when pdo_mysql extension with mysqlnd driver, if the third party is allowed to supply host to connect to and the password for the connection, password of excessive length can trigger a buffer overflow in PHP, which can lead to a remote code execution vulnerability.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31626>
- CVE-2022-31625
In PHP versions 7.4.x below 7.4.30, 8.0.x below 8.0.20, and 8.1.x below 8.1.7, when using Postgres database extension, supplying invalid parameters to the parametrized query may lead to PHP attempting to free memory using uninitialized data as pointers. This could lead to RCE vulnerability or denial of service.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31625>
- CVE-2022-31374
An arbitrary file upload vulnerability /images/background/1.php in of SolarView Compact 6.0 allows attackers to execute arbitrary code via a crafted php file.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31374>
- CVE-2022-31158
LTI1.3 Tool Library is a library used for building IMS-certified LTI1.3 tool providers in PHP. Prior to version 5.0

Back

Windows 10&11

Microsoft의 운영체제이다.

Windows 10,11

- CVE-2022-36415
A DLL hijacking vulnerability exists in the uninstaller in Scooter Beyond Compare 1.8a through 4.4.2 before 4.4.3 when installed via the EXE installer. The uninstaller attempts to load DLLs out of a Windows Temp folder. If a standard user places malicious DLLs in the C:\Windows\Temp\ folder, and then the uninstaller is run as SYSTEM, the DLLs will execute with elevated privileges.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36415>
- CVE-2022-36414
There is an elevation of privilege breakout vulnerability in the Windows EXE installer in Scooter Beyond Compare 4.2.0 through 4.4.2 before 4.4.3. Affected versions allow a logged-in user to run applications with elevated privileges via the Clipboard Compare tray app after installation.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36414>
- CVE-2022-34866
Passage Drive versions v1.4.0 to v1.5.1.0 and Passage Drive for Box version v1.0.0 contain an insufficient data verification vulnerability for interprocess communication. By running a malicious program, an arbitrary OS command may be executed with LocalSystem privilege of the Windows system where the product is running.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34866>
- CVE-2022-34006
An issue was discovered in TitanFTP (aka Titan FTP) NextGen before 1.2.1050. When installing, Microsoft SQL Express 2019 installs by default with an SQL instance running as SYSTEM with BUILTIN\Users as sysadmin, thus enabling unprivileged Windows users to execute commands locally as NT AUTHORITY\SYSTEM, aka NX-1674 (sub-issue 2). NOTE: as of 2022-06-21, the 1.2.1050 release corrects this vulnerability in a new installation, but not in an upgrade installation.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34006>
- CVE-2022-33711
Improper validation of integrity check vulnerability in Samsung USB Driver Windows Installer for Mobile Phones prior to version 1.7.56.0 allows local attackers to delete arbitrary directory using directory junction.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33711>
- CVE-2022-33127
The function that calls the diff tool in Diffy 3.4.1 does not properly handle double quotes in a filename when run in a windows environment. This allows attackers to execute arbitrary commands via a crafted string.
<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33127>
- CVE-2022-32236
When a user opens manipulated Windows Bitmap (.bmp, 2d.x3d) files received from untrusted sources in

Back

0-Day Twitter News

- <https://twitter.com/binitamshah>
- <https://twitter.com/DirectoryRanger>
- <https://twitter.com/campuscodi>
- <https://twitter.com/Dinosn>
- https://twitter.com/malware_traffic
- <https://twitter.com/holisticinfosec>
- <https://twitter.com/DissectMalware>
- <https://riskybiznews.substack.com/>

- Crawler 실행
- 검색어 입력
- DB 저장
- Slack 및 Web 으로 전달

The screenshot displays a Windows desktop environment with several open applications:

- Visual Studio Code:** The main window shows a Python script named `cr_slack.py` with the following code:

```
def tw_data_table():  
    #show  
    conn = pymysql.connect(host='127.0.0.1',user='root',password='park10')  
    cursor = conn.cursor()  
    table_creat123 = '''CREATE TABLE tw_all_data (  
        id int(11) NOT NULL AUTO_INCREMENT PRIMARY KEY,  
        tw_data varchar(1200),  
        link varchar(600)  
    )  
    '''  
    time.sleep(2)  
    cursor.execute(table_creat123)  
    conn.commit()  
  
    ''' sho = 'SELECT tw_link FROM tw_url_list'  
    cursor.execute(sho)  
    result120 = cursor.fetchall()  
    result1 = list(result120)  
    print(result1) '''  
    conn.close()  
    save_tw_url()  
  
def save_tw_url():  
    print('tw_data_save 시작')  
  
    conn = pymysql.connect(host='127.0.0.1',user='root',password='park10')  
    cursor = conn.cursor()  
  
    show = 'SELECT tw_link FROM tw_url_list'  
    cursor.execute(show)  
    result = cursor.fetchall()  
    print(result)  
  
    # 종합 보안 뉴스 트윗  
    s_news1 = 'https://twitter.com/binitamshah'  
    s_news2 = 'https://twitter.com/DirectoryRanger.'  
    s_news3 = 'https://twitter.com/campuscodi'  
    s_news4 = 'https://twitter.com/Dinosn'
```
- Bandicam:** A recording window is overlaid on the code editor, showing a timer at 00:00:00 and various recording controls. The settings panel is open, showing the save path as `C:\Users\wsbie\Documents\Bandicam`.
- Slack:** A chat window is visible in the background, showing a message input field with the text `show link?` and a `Click Me` button.

The Windows taskbar at the bottom shows the system tray with the date and time: `오전 9:24 2022-07-28`.

PROCESS

Demo - Bot act

14

CVE_BOT 앱 오후 5:27
AD서버 취약점입니다
Content : A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.
Number : CVE-2022-30190
Link : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190>

어제 ~

CVE_BOT 앱 오전 12:09
CVE-2022-30190
A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.
Link : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190>

CVE-2022-25154
A DLL hijacking vulnerability in Samsung portable SSD T5 PC software before 1.6.9 could allow a local attacker to escalate privileges. An attacker must already have user privileges on Windows 7, 10, or 11 to exploit this vulnerability.
Link : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25154>

CVE_BOT 앱 오전 12:16
CVE-2022-34965
OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component /ossn/administrator/com_installer. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.
Link : <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34965>

Test

Vuln Bot 앱 오전 4:38
New vulnerability information.
CVE-2022-36415
A DLL hijacking vulnerability exists in the uninstaller in Scooter Beyond Compare 1.8a through 4.4.2 before 4.4.3 when installed via the EXE installer. The uninstaller attempts to load DLLs out of a Windows Temp folder. If a standard user places malicious DLLs in the C:\Windows\Temp\ folder, and then the uninstaller is run as SYSTEM, the DLLs will execute with elevated privileges.
간략히 보기
2022-07-28 04:38:35
상세한 내용은 자세히 보기를 클릭해주세요. 자세히 보기

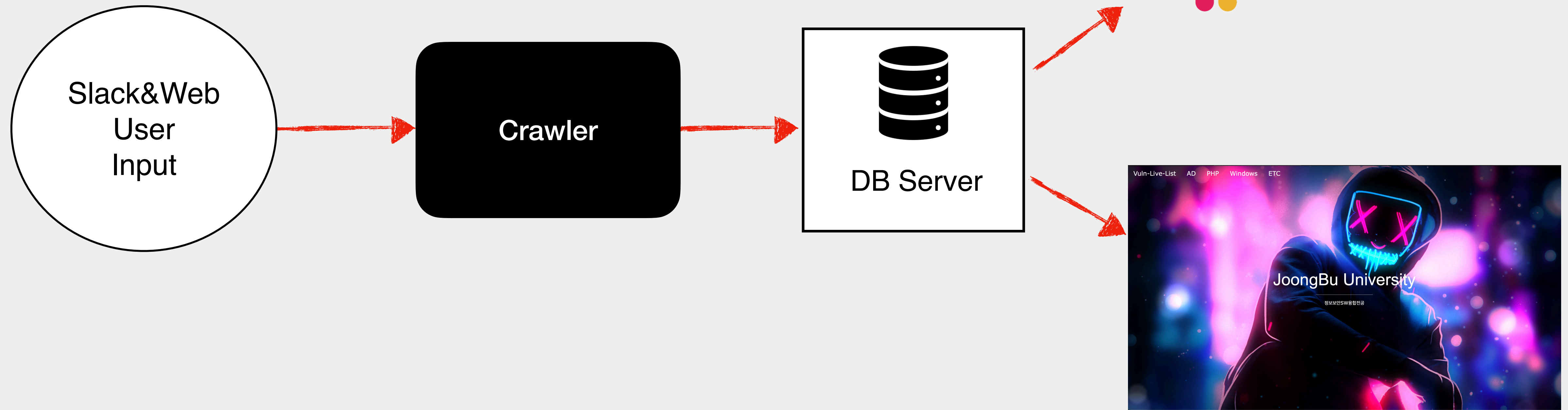
New vulnerability information.
CVE-2022-36900
Jenkins Compuware zAdviser API Plugin 1.0.3 and earlier does not restrict execution of a controller/agent message to agents, allowing attackers able to control agent processes to retrieve Java system properties.
간략히 보기
2022-07-28 04:39:12
상세한 내용은 자세히 보기를 클릭해주세요. 자세히 보기

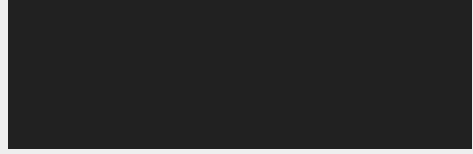
New vulnerability information.
CVE-2022-26034

Final

MyslackBot 앱 오전 8:24
CVE_LIST 검색 결과.
CVE-2022-34971
Great to see you here! App helps you to stay up-to-date with your meetings and events right here within Slack. These are just a few things which you will be able to do:
An arbitrary file upload vulnerability in the Advertising Management module of Feehi CMS v2.1.1 allows attackers to execute arbitrary code via a crafted PHP file.
show link? Click Me

MyslackBot 앱 오전 7:29
test 메시지를 보냅니다.
메인 트윗
Binni Shah
@binitamshah
·
7시간
더 보기
Great to see you here! App helps you to stay up-to-date with your meetings and events right here within Slack. These are just a few things which you will be able to do:
Binni Shah
@binitamshah
·
7시간
Awesome RCE techniques : Awesome list of techniques to achieve Remote Code Execution (RCE) on various apps! : <https://github.com/p0dalirius/Awesome-RCE-techniques...> credits
더 보기
show link? Click Me







- CVE 하단에 관련 정보 #태그
- Side-Bar 검색
- 공개된 POC(GitHub) 링크 하단에 출력

PROCESS

QnA

18

Q n A